코드인스펙션 도구 POC 테스트결과

I. 코드 인스펙션 POC 전체 현황

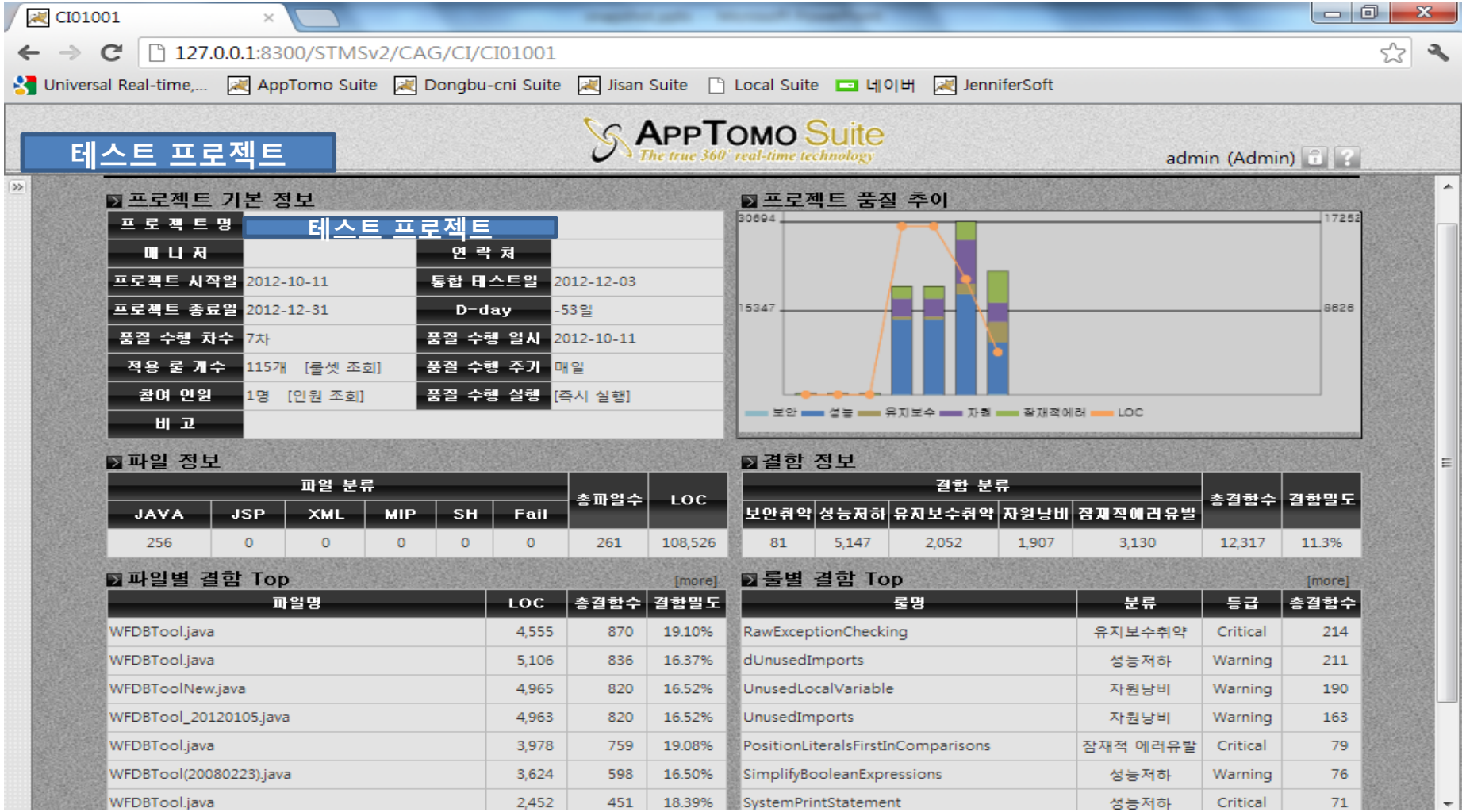
■ Java Code 점검 현황 (점검 규칙 : 115개 Rule)

AppTomo			Code Prism			Sonar		
보안취약	126	0.02%	필 수	295	0.04%	심 각	96	0.012%
성능저하	22,651	2.71%	권고-상	17,868	2.14%	메이저	29,040	3.48%
유지보수취약	3,408	0.41%	권고-중	4,738	0.57%	마이너	209,542	25.11%
자원낭비	8,072	0.97%	권고-하	15,583	1.87%	권 고	12	0.00%
잠재에러유발	6,120	0.73%			0.00%			0.00%
총 결함수	40,377	4.84%	총 결함수	38,484	4.61%	총 결함수	238,690	29%

패키지별 POC 현황

II. 패키지별 POC 현황 – AppTomo

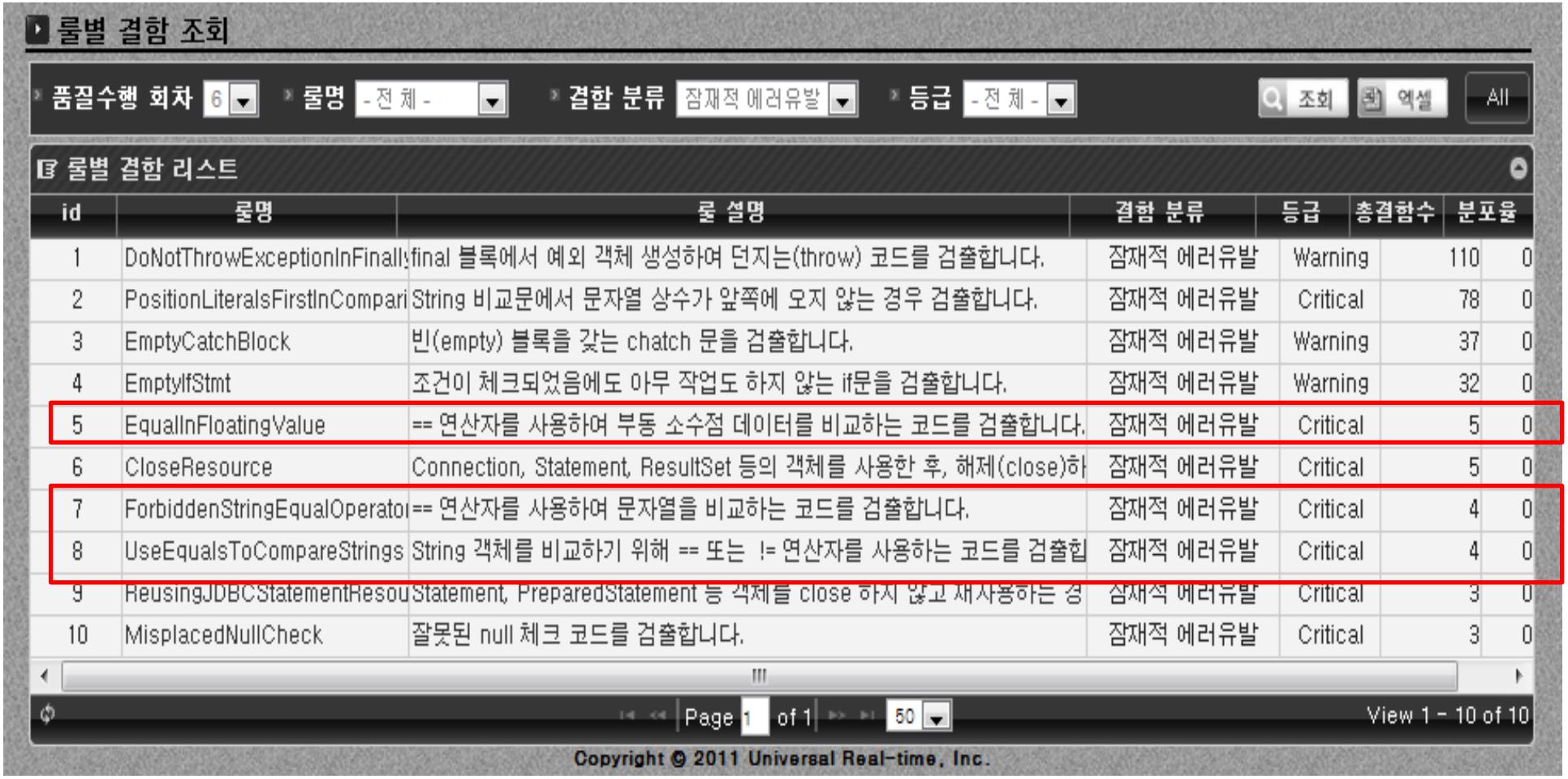
❖ 자바 업무 샘플 - 3



II. 패키지별 POC 현황 – AppTomo

❖ 자바 업무 샘플 - 3

● 잠재 에러 유발 유형



룰별 결함 조회

품질수행 회차 6 | 룰명 - 전 체 - | 결함 분류 잠재적 에러유발 | 등급 - 전 체 - | 조회 | 엑셀 | All

룰별 결함 리스트

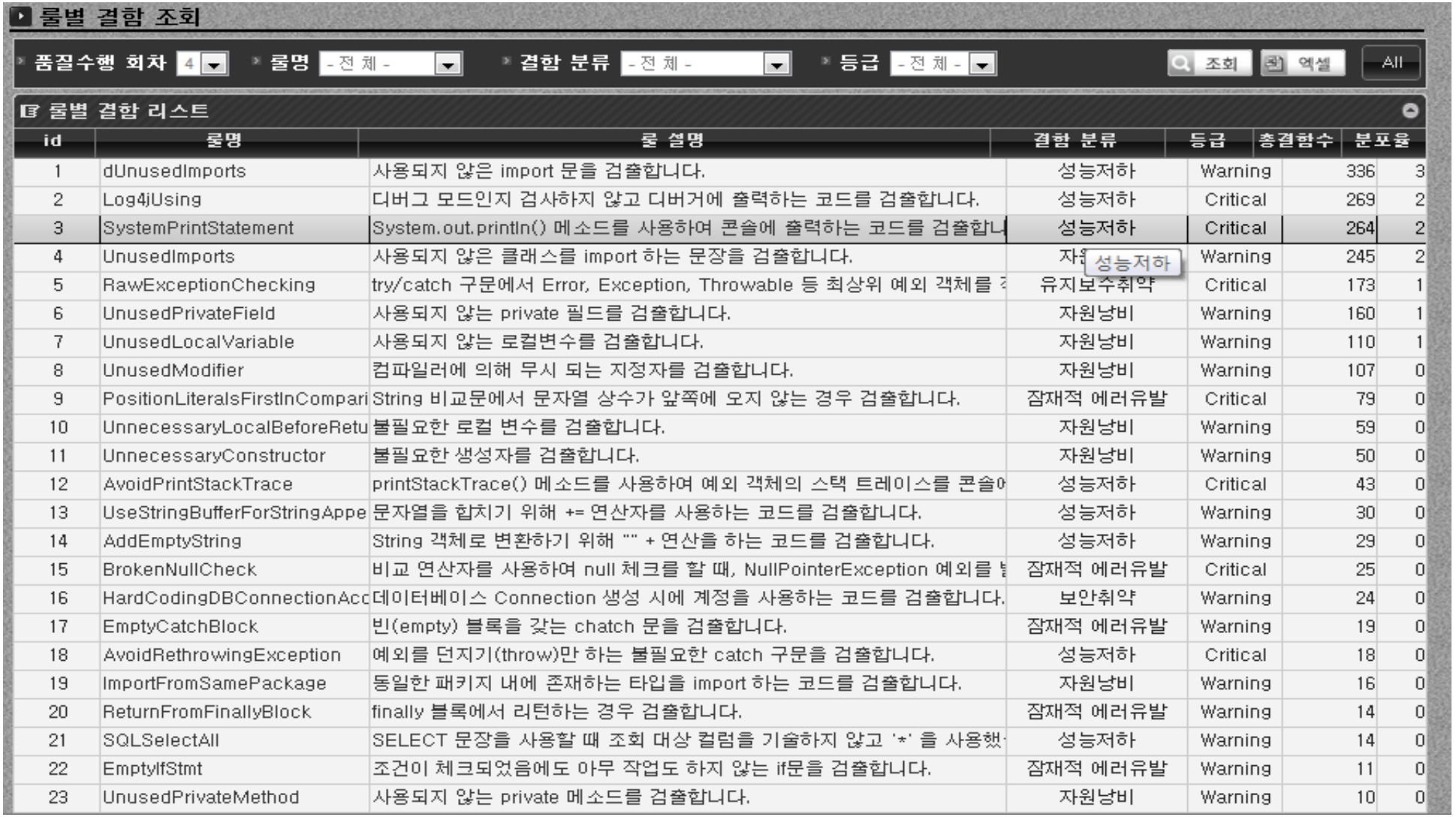
id	룰명	룰 설명	결함 분류	등급	총결함수	분포율
1	DoNotThrowExceptionInFinally	final 블록에서 예외 객체 생성하여 던지는(throw) 코드를 검출합니다.	잠재적 에러유발	Warning	110	0
2	PositionLiteralsFirstInCompari	String 비교문에서 문자열 상수가 앞쪽에 오지 않는 경우 검출합니다.	잠재적 에러유발	Critical	78	0
3	EmptyCatchBlock	빈(empty) 블록을 갖는 chatch 문을 검출합니다.	잠재적 에러유발	Warning	37	0
4	EmptyIfStmt	조건이 체크되었음에도 아무 작업도 하지 않는 if문을 검출합니다.	잠재적 에러유발	Warning	32	0
5	EqualInFloatingValue	== 연산자를 사용하여 부동 소수점 데이터를 비교하는 코드를 검출합니다.	잠재적 에러유발	Critical	5	0
6	CloseResource	Connection, Statement, ResultSet 등의 객체를 사용한 후, 해제(close)하	잠재적 에러유발	Critical	5	0
7	ForbiddenStringEqualOperator	== 연산자를 사용하여 문자열을 비교하는 코드를 검출합니다.	잠재적 에러유발	Critical	4	0
8	UseEqualsToCompareStrings	String 객체를 비교하기 위해 == 또는 != 연산자를 사용하는 코드를 검출힙	잠재적 에러유발	Critical	4	0
9	ReusingJDBCStatementResou	Statement, PreparedStatement 등 객체를 close 하지 않고 재사용하는 경	잠재적 에러유발	Critical	3	0
10	MisplacedNullCheck	잘못된 null 체크 코드를 검출합니다.	잠재적 에러유발	Critical	3	0

Page 1 of 1 | 50 | View 1 - 10 of 10

Copyright © 2011 Universal Real-time, Inc.

II. 패키지별 POC 현황 – AppTomo

❖ Rule 위반 유형



룰별 결함 조회

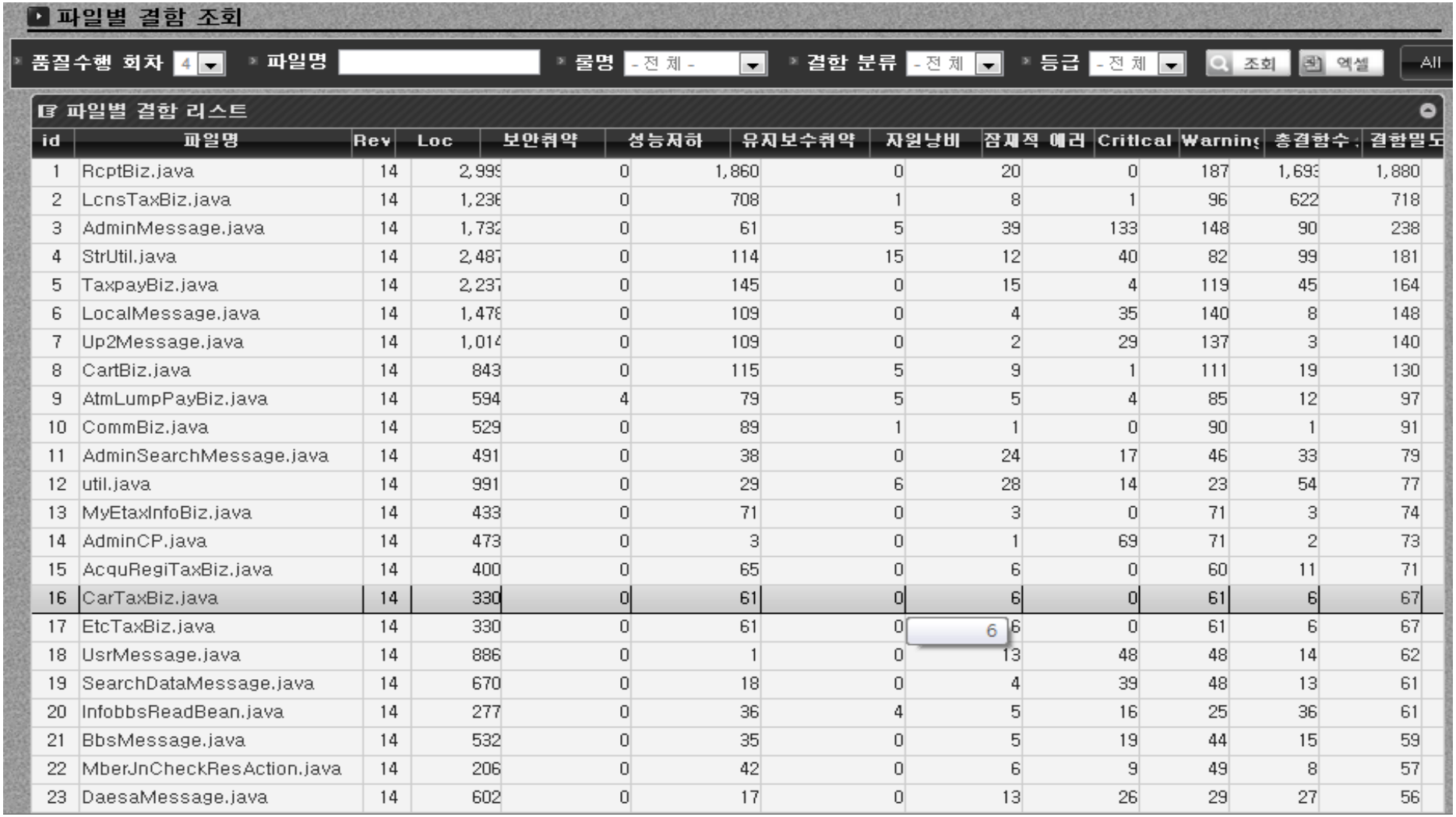
품질수행 회차 4 | 룰명 - 전 체 - | 결함 분류 - 전 체 - | 등급 - 전 체 - | 조회 | 엑셀 | All

룰별 결함 리스트

id	룰명	룰 설명	결함 분류	등급	총결함수	분포율
1	dUnusedImports	사용되지 않은 import 문을 검출합니다.	성능저하	Warning	336	3
2	Log4jUsing	디버그 모드인지 검사하지 않고 디버거에 출력하는 코드를 검출합니다.	성능저하	Critical	269	2
3	SystemPrintStatement	System.out.println() 메소드를 사용하여 콘솔에 출력하는 코드를 검출합니	성능저하	Critical	264	2
4	UnusedImports	사용되지 않은 클래스를 import 하는 문장을 검출합니다.	자원	Warning	245	2
5	RawExceptionChecking	try/catch 구문에서 Error, Exception, Throwable 등 최상위 예외 객체를	유지보수취약	Critical	173	1
6	UnusedPrivateField	사용되지 않는 private 필드를 검출합니다.	자원낭비	Warning	160	1
7	UnusedLocalVariable	사용되지 않는 로컬변수를 검출합니다.	자원낭비	Warning	110	1
8	UnusedModifier	컴파일러에 의해 무시 되는 지정자를 검출합니다.	자원낭비	Warning	107	0
9	PositionLiteralsFirstInCompari	String 비교문에서 문자열 상수가 앞쪽에 오지 않는 경우 검출합니다.	잠재적 에러유발	Critical	79	0
10	UnnecessaryLocalBeforeRetu	불필요한 로컬 변수를 검출합니다.	자원낭비	Warning	59	0
11	UnnecessaryConstructor	불필요한 생성자를 검출합니다.	자원낭비	Warning	50	0
12	AvoidPrintStackTrace	printStackTrace() 메소드를 사용하여 예외 객체의 스택 트레이스를 콘솔에	성능저하	Critical	43	0
13	UseStringBufferForStringAppe	문자열을 합치기 위해 += 연산자를 사용하는 코드를 검출합니다.	성능저하	Warning	30	0
14	AddEmptyString	String 객체로 변환하기 위해 "" + 연산을 하는 코드를 검출합니다.	성능저하	Warning	29	0
15	BrokenNullCheck	비교 연산자를 사용하여 null 체크를 할 때, NullPointerException 예외를	잠재적 에러유발	Critical	25	0
16	HardCodingDBConnectionAcc	데이터베이스 Connection 생성 시에 계정을 사용하는 코드를 검출합니다.	보안취약	Warning	24	0
17	EmptyCatchBlock	빈(empty) 블록을 갖는 chatch 문을 검출합니다.	잠재적 에러유발	Warning	19	0
18	AvoidRethrowingException	예외를 던지기(throw)만 하는 불필요한 catch 구문을 검출합니다.	성능저하	Critical	18	0
19	ImportFromSamePackage	동일한 패키지 내에 존재하는 타입을 import 하는 코드를 검출합니다.	자원낭비	Warning	16	0
20	ReturnFromFinallyBlock	finally 블록에서 리턴하는 경우 검출합니다.	잠재적 에러유발	Warning	14	0
21	SQLSelectAll	SELECT 문장을 사용할 때 조회 대상 컬럼을 기술하지 않고 '*' 을 사용했	성능저하	Warning	14	0
22	EmptyIfStmt	조건이 체크되었음에도 아무 작업도 하지 않는 if문을 검출합니다.	잠재적 에러유발	Warning	11	0
23	UnusedPrivateMethod	사용되지 않는 private 메소드를 검출합니다.	자원낭비	Warning	10	0

II. 패키지별 POC 현황 – AppTomo

❖ 프로그램별 코드 품질 샘플



파일별 결함 조회

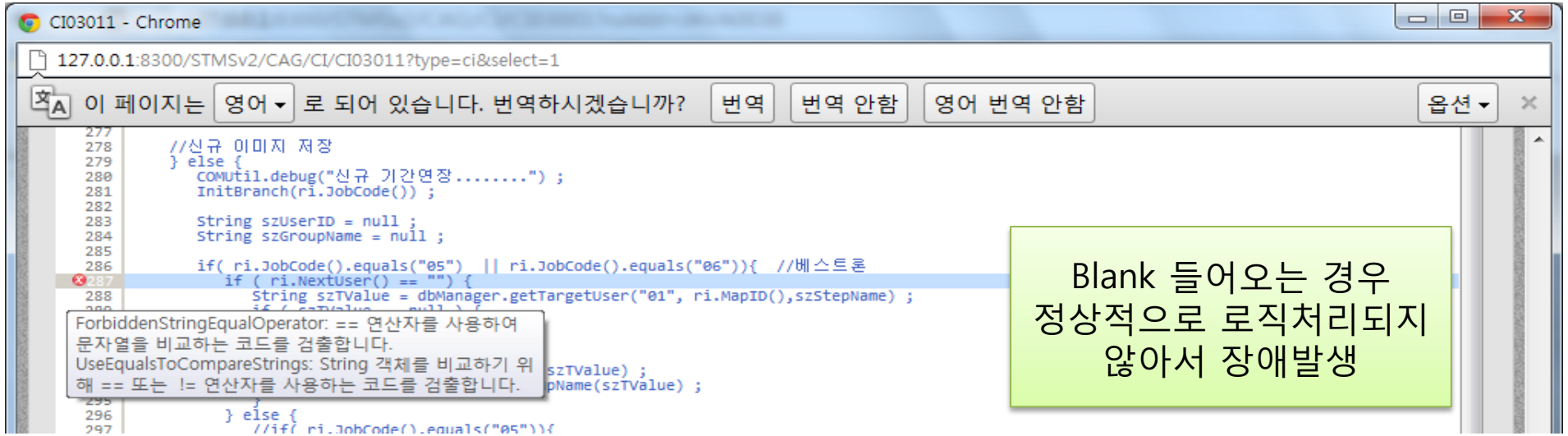
품질수행 회차 4 | 파일명 | 룰명 - 전 체 - | 결함 분류 - 전 체 | 등급 - 전 체 | 조회 | 엑셀 | All

파일별 결함 리스트

id	파일명	Rev	Loc	보안취약	성능저하	유지보수취약	자원낭비	잠재적 에러	Critical	Warning	총결함수	결함밀도
1	RcptBiz.java	14	2,999	0	1,860	0	20	0	187	1,693	1,880	
2	LcnsTaxBiz.java	14	1,236	0	708	1	8	1	96	622	718	
3	AdminMessage.java	14	1,732	0	61	5	39	133	148	90	238	
4	StrUtil.java	14	2,487	0	114	15	12	40	82	99	181	
5	TaxpayBiz.java	14	2,237	0	145	0	15	4	119	45	164	
6	LocalMessage.java	14	1,478	0	109	0	4	35	140	8	148	
7	Up2Message.java	14	1,014	0	109	0	2	29	137	3	140	
8	CartBiz.java	14	843	0	115	5	9	1	111	19	130	
9	AtmLumpPayBiz.java	14	594	4	79	5	5	4	85	12	97	
10	CommBiz.java	14	529	0	89	1	1	0	90	1	91	
11	AdminSearchMessage.java	14	491	0	38	0	24	17	46	33	79	
12	util.java	14	991	0	29	6	28	14	23	54	77	
13	MyEtaxInfoBiz.java	14	433	0	71	0	3	0	71	3	74	
14	AdminCP.java	14	473	0	3	0	1	69	71	2	73	
15	AcquRegiTaxBiz.java	14	400	0	65	0	6	0	60	11	71	
16	CarTaxBiz.java	14	330	0	61	0	6	0	61	6	67	
17	EtcTaxBiz.java	14	330	0	61	0	6	0	61	6	67	
18	UsrMessage.java	14	886	0	1	0	13	48	48	14	62	
19	SearchDataMessage.java	14	670	0	18	0	4	39	48	13	61	
20	InfobbsReadBean.java	14	277	0	36	4	5	16	25	36	61	
21	BbsMessage.java	14	532	0	35	0	5	19	44	15	59	
22	MberJnCheckResAction.java	14	206	0	42	0	6	9	49	8	57	
23	DaesaMessage.java	14	602	0	17	0	13	26	29	27	56	

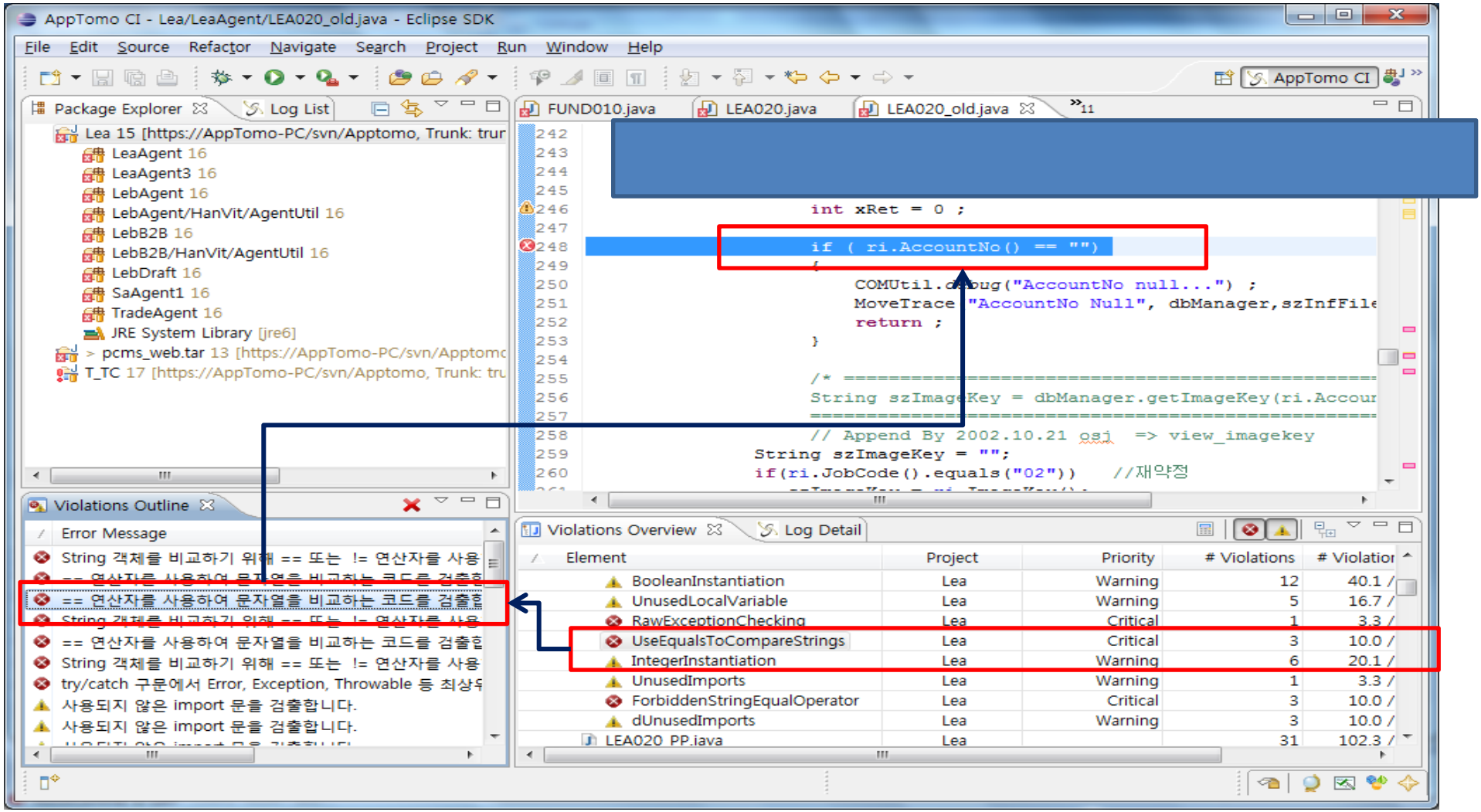
II. 패키지별 POC 현황 – AppTomo

❖ 주요 룰 위반 점검 (관리자 지원)



II. 패키지별 POC 현황 – AppTomo

❖ 주요 룰 위반 점검 (개발자 자가 품질진단)



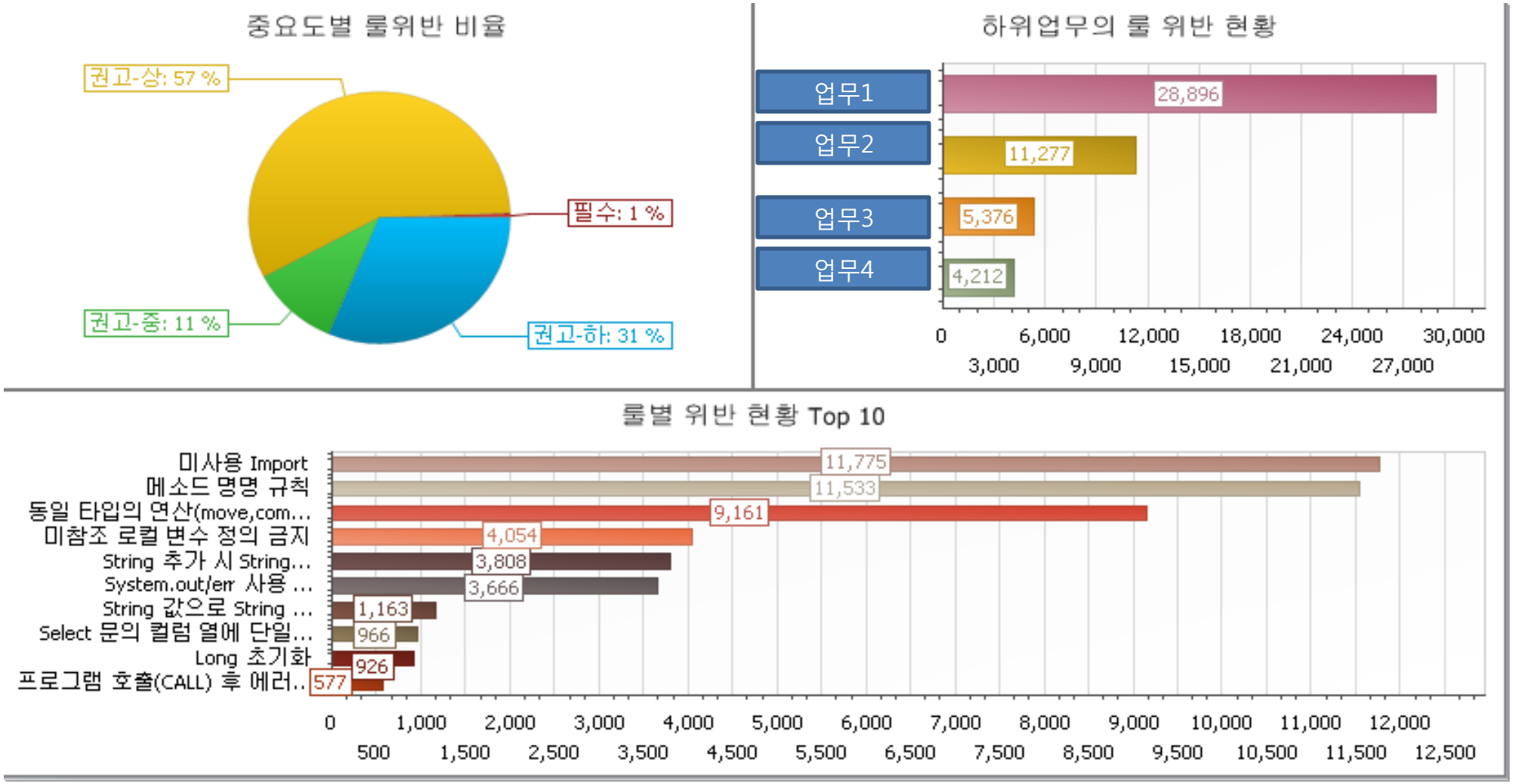
II. 패키지별 POC 현황 – AppTomo

❖ 주요 룰 위반 점검 (개발자 자가 품질진단 – 개발자 가이드)

패키지별 POC 현황
- CodePrism

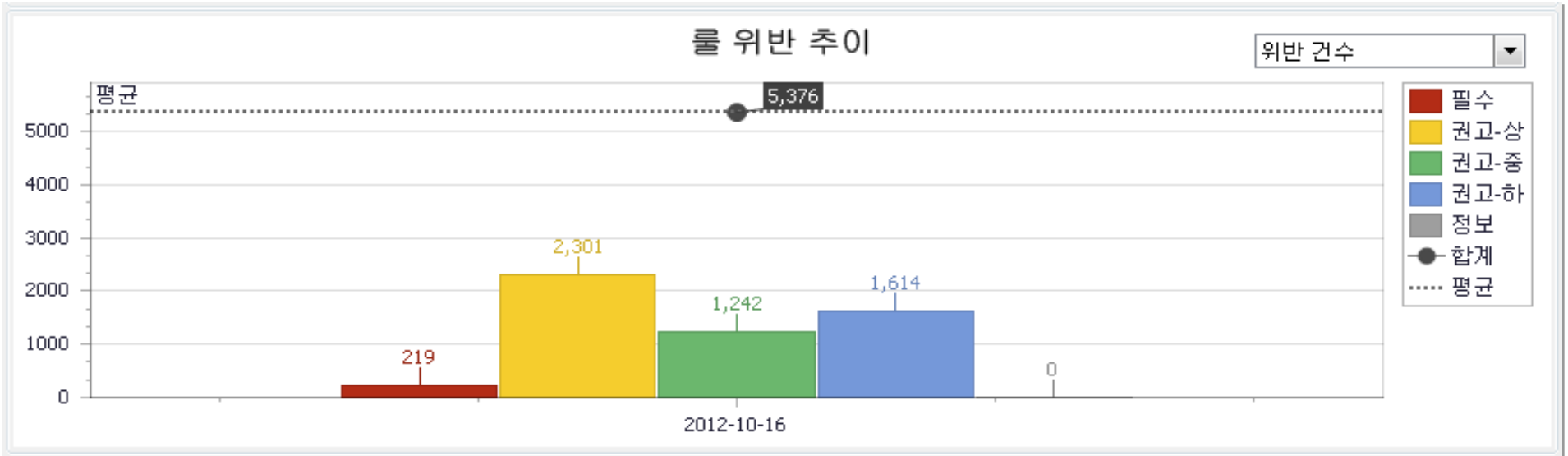
III. 패키지별 POC 현황 – CodePrism

❖ 전체 Rule 위반 현황



III. 패키지별 POC 현황 – CodePrism

❖ Java 샘플 -1 위반현황



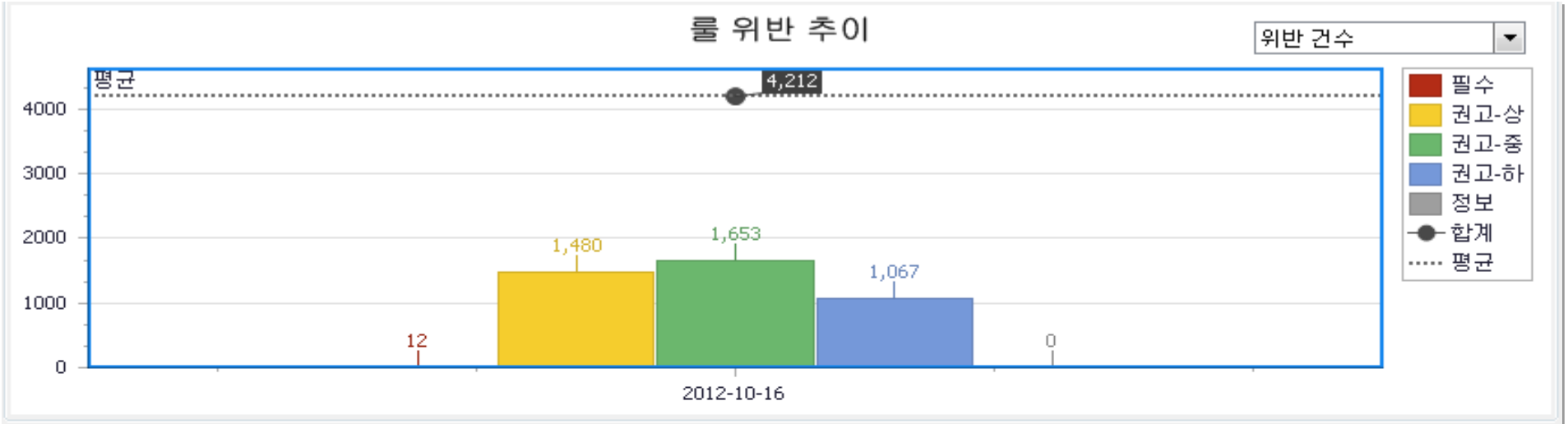
목록 | 비교

2012-10-16 모두

우선순위	카테고리	룰 이름	위반 건수	위반 파일 건수
필수	PMD->기본->불완전한 Null 검사	불완전한 Null 검사	1	1
필수	SQL->코딩표준->성능->INSERT 문...	INSERT 문에서 컬럼과 입력값의 개수 일치	12	2
필수	공통->표준화->하드코딩->IP 주소...	IP 주소의 하드코딩 금지	194	20
필수	공통->표준화->하드코딩->주민등록...	주민등록번호 하드코딩 금지	5	5
필수	언어별지원->최적화->자원누수->D...	DB 자원 해제 검사	4	1
권고-상	PMD->Java Logging->System.out/e...	System.out/err 사용 금지	338	71
권고-상	PMD->기본->Boolean 값으로 Boolea...	Boolean 값으로 Boolean 인스턴스 생성 금지 (Boole...	6	6

III. 패키지별 POC 현황 – CodePrism

❖ Java 샘플 -3 위반현황



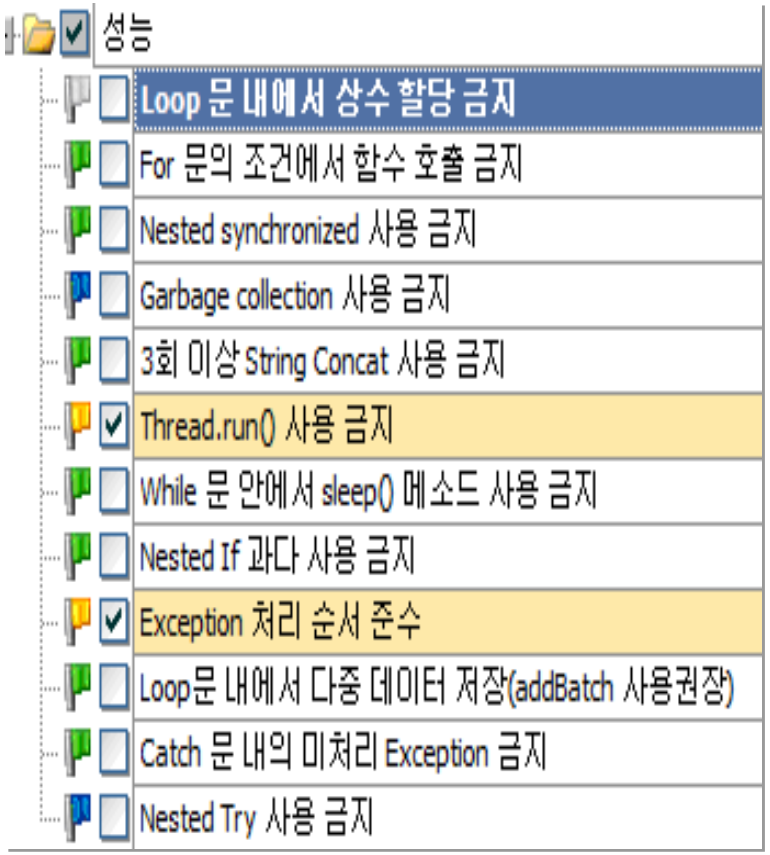
목록 | 비교

2012-10-16 모두

우선순위	카테고리	룰 이름	위반 건수	위반 파일 건수
필수	SQL->코딩표준->성능->INSERT 문...	INSERT 문에서 컬럼과 입력값의 개수 일치	4	1
필수	공통->표준화->하드코딩->IP 주소...	IP 주소의 하드코딩 금지	4	2
필수	언어별지원->최적화->자원누수->D...	DB 자원 해제 검사	4	2
권고-상	PMD->Java Logging->System.out/e...	System.out/err 사용 금지	1,036	80
권고-상	PMD->Strict Exception->자체 Exce...	자체 Exception 타입 Throw 금지	125	6
권고-상	PMD->명명규칙->메소드 명명 규칙	메소드 명명 규칙	319	60
권고-중	PMD->디자인->객체 비교시 '==' 연...	객체 비교시 '==' 연산자 사용 금지	25	9

III. 패키지별 POC 현황 – CodePrism

❖ 주요 Rule 유형



III. 패키지별 POC 현황 – CodePrism

❖ Critical Rule 위반 사례

* System.out, err등을 사용하며 해킹의 대상이 될 수 있어 사용을 금지 (CWE 398). ➔ 보안규칙

● Java

```
78              VidVerifier vid = new VidVerifier(xecConfig);
79
80              System.out.println("dn : "+ dn);
81              System.out.println("sn : "+ sn);
82              System.out.println("jumin_no"+ StrUtil.evl(xRequest.getParameter("jumin_no"), ""));
83              System.out.println("bubin_no"+ StrUtil.evl(xRequest.getParameter("bubin_no"), ""));
84
85              //inputDto.setDn(dn);
86              //inputDto.setSn(sn);
87
88              String idn = StrUtil.evl(inputDto.getNap_id(), "");
89
90  //          if("".equals(idn)){
```

룰 위반 보기 - 서울시서비스부

위반 라인	경로
필수 (64)	
권고-상 (14087)	
Integer 초기화 (23)	
Long 초기화 (926)	
String 값으로 String 인스턴스 생성 금지 (1163)	
System.out/err 사용 금지 (2292)	
AcquRegiTaxProxRegiInptAction.java (7)	
80	/pcms_web/
81	/pcms_web/
82	/pcms_web/
83	/pcms_web/

검색 결과 | 룰 위반 보기 - 서울시서비스부

룰 설명 - AcquRegiTaxProxRegiInptAction.java

룰 이름	System.out/err 사용 금지
우선순위	권고-상

설명 | 예제

표준 출력/에러인 System.out.println()/System.err.println()을 사용하지 않도록 권고합니다.

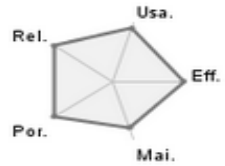
[참고] 애플리케이션은 다양한 문제들로 인해 의도하지 않게 설정 정보, 내부 작업 내용, 개인 정보 등을 유출할 수 있습니다. 해커들은 이런 약점을 이용해 민감한 데이터를 가로채거나 보다 심각한 공격을 감행할 수 있습니다. (OWASP Top 10: A7 Improper Error Handling / CWE 398: Indicator of Poor Code Quality)

패키지별 POC 현황
- Sonar (오픈소스)

IV. 패키지별 POC 현황 – Sonar

❖ Java 위반현황 - 샘플 1

Rules compliance
71.5%



Violations
13,883

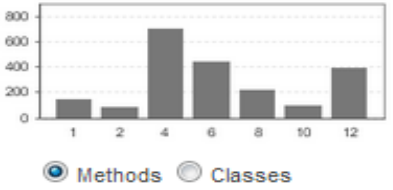
Blocker	0	
Critical	96	
Major	13,170	
Minor	605	
Info	12	

Events All

2012/10/12	Version	17	Edit Delete
2012/10/12	Version	16	Edit Delete
2012/10/12	Version	15	Edit Delete
2012/10/12	Version	14	Edit Delete

Add an event

Complexity
11.2 / method
109.0 / class
109.0 / file
Total: 22,997



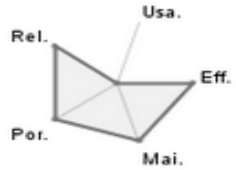
Technical Debt
61.3%
$ 6,674,575
13,349 man days

No information available on coverage

IV. 패키지별 POC 현황 – Sonar

❖ Java 위반 현황 - 샘플 2

Rules compliance
0.0%



Violations
37,274

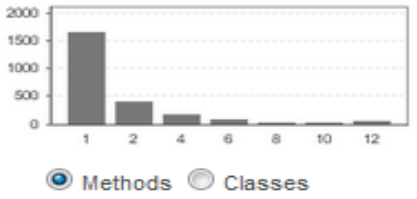
Blocker	0	
Critical	0	
Major	6,827	
Minor	30,447	
Info	0	

Events All

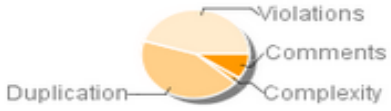
2012/10/12	Version	2	Edit Delete
2012/10/12	Version	3	Edit Delete
2012/10/12	Version	1	Edit Delete

Add an event

Complexity
2.1 / method
22.2 / class
22.2 / file
Total: 5,062



Technical Debt
45.9%
$ 517,175
1,034 man days

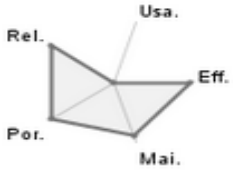


No information available on coverage

IV. 패키지별 POC 현황 – Sonar

❖ Java 위반 현황 - 샘플 3

Rules compliance
0.0%



Violations
187,533

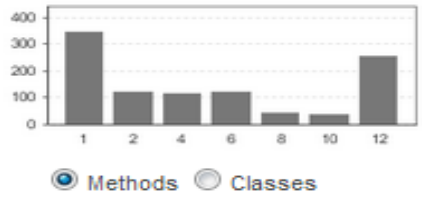
Blocker	0	
Critical	0	
Major	9,043	
Minor	178,490	
Info	0	

Events All

2012/10/12	Version	4	Edit Delete

Add an event

Complexity
7.7 / method
61.1 / class
65.9 / file
Total: 12,652



Technical Debt
148.5%
$ 1,667,738
3,336 man days

No information available on coverage

IV. 패키지별 POC 현황 – Sonar

❖ Java 주요 위반 현황

Empty Catch Block : 104건
- com.woori.tc.plan.ProcIaoBssLstDAO : 239 라인
  }**catch** (SQLException e) { **(오류처리 하지 않음)**

Empty If Stmt : 77건
- com.woori.tc.ifrs.ProcIfrsIncreaseRateEJB : 363 라인
  }**else**{ **(Else 실행문 없음)**

Empty Finally Block : 19건
- com.woori.tc.plan.ProcEValuationEJB : 2616 라인
  } **finally { (Finally 실행문 없음)**

Misplaced Null Check : 4건
- com.woori.tc.plan.ProcDBSisanReqPopEJB : 67.,70 라인
  if (op.equals(**"T_S"**)||op == **null**) { **(op가 null일 경우 오류발생)**
  }**else if** (op.equals(**"X_Q"**)||op == **null**) {

NPath complexity : 229 건
- com.woori.tc.plan.ProcEValuationEJB : 3722 라인 **(로직이 너무 복잡함 – 분할 필요**)
  public boolean eValuation_JIYUL_READ(**double** ***SUPPLY_SEQ_NUM***, String ***PAYTYPE_STD***, String ***CHANGE_IND***) **throws** AppEJBException, AppException {

Empty While Stmt : 13건
- while(bWait == false) { } **(무한루프에 빠질 가능성 있음)**

- 일반적인 Rule 위반 정제 필요
- 오류에 대한 가이드 미 제공